On the incompatibility of noncommuting observables

Somshubhro Bandyopadhyay
Department of Physics and Center for Astroparticle Physics and Space Science, Bose Institute, Block EN, Sector V, Bidhan Nagar, Kolkata 700091, India *

Prabha Mandayam
The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India †

Uncertainty relations are often considered to be a measure of incompatibility of noncommuting observables. However, such a consideration is not valid in general, motivating the need for an alternate measure that applies to any set of noncommuting observables. We present an operational approach to quantifying incompatibility without invoking uncertainty relations. Our measure aims to capture the incompatibility of noncommuting observables as manifest in the non-orthogonality of their eigenstates. We prove that this measure has all the desired properties: it is zero when the observables commute, strictly greater than zero when they do not, and is maximum when they are mutually unbiased. We also obtain tight upper bounds on this measure for any N noncommuting observables and compute it exactly when the observables are mutually unbiased.

In quantum theory, any observable or a set of commuting observables can in principle be measured with any desired precision. This is because commuting observables have a complete set of simultaneous eigenkets, and therefore, measurement of one does not disturb the measurement result obtained for the other. This no longer holds when the observables do not commute. noncommuting observables do not have a complete set of common eigenkets, and therefore it is impossible to specify definite values simultaneously. This is the essence of the celebrated uncertainty principle [1, 2]. Uncertainty relations [1–4, 6–16, 20] express the uncertainty principle in a quantitative way by providing a lower bound on the "uncertainty" in the result of a simultaneous measurement of noncommuting observables.

Observables are defined to be compatible when they commute, and incompatible when they do not. The uncertainty principle, therefore, is a manifestation of the incompatibility of noncommuting observables. Despite the conceptual importance of incompatible observables and applications of such observables in quantum state determination [33–35] and quantum cryptography [25, 26, 28–30], there does not seem to be a good general measure of their incompatibility, although entropic uncertainty relations have often been considered for this purpose (see for example, [15, 17–19]).

To see in what sense uncertainty relations quantify incompatibility of noncommuting observables, consider, for example, the entropic uncertainty relation due to Maassen and Uffink [4]. For any quantum state $\rho \in \mathscr{H}$ with $\dim \mathscr{H} = d$, and measurement of any two observables A and B with eigenvectors $\{|a_i\rangle\}$ and $\{|b_i\rangle\}$ respectively, it was shown that [4]

$$\frac{1}{2}\left(H(A|\rho)+H(B|\rho)\right) \;\geq\; -\log c, \qquad (1)$$

where $c = \max |\langle a|b\rangle|$: $|a\rangle \in \{|a_i\rangle\}, |b\rangle \in \{|b_i\rangle\}$, and $H(X|\rho) = -\sum_{i=1}^{d} \langle x_i|\rho|x_i\rangle \log \langle x_i|\rho|x_i\rangle$ for $X \in \{A,B\}$ is the Shannon entropy. Observe that the right hand side of the above inequality is ρ independent. The incompatibility of the observables A and B can be measured by either the sum of the entropies [left hand side of (1)] minimized over all ρ (if it is not known whether equality is achieved), or the lower bound when the equality is achieved for some state. We then say that a set of observables is more incompatible than another if the sum (or the lower bound) takes on a larger value. It is clear from the above inequality that a pair of observables is most incompatible when the observables are mutually unbiased. Incompatibility of more than two observables can be similarly quantified via a generalized form of the inequality (1) [15] when such an inequality can be found.

However, it is easy to see why inequality (1) is not a satisfactory measure of incompatibility for *all* pairs of incompatible observables. This is because both sides of the inequality could be zero even when the observables do not commute. This happens, for example, when the noncommuting observables A and B are such that they commute on a subspace. Such observables have one or more common eigenvectors but not all eigenvectors are common because the observables do not commute. For such a pair of observables both sides of inequality (1) are identically zero even though the observables are known to be incompatible. Thus uncertainty relations can only quantify incompatibility when the observables do not have any common eigenvector. This shows that uncertainty relations cannot be considered as a valid measure of incompatibility for *all* sets of noncommuting observables, thus motivating the present work. Furthermore, incompatibility of more than two observables is much less understood because uncertainty relations (in cases where they are indeed a good measure) are known only for some special classes of observables [11–13, 16, 20]. Even for these cases maximally tight uncertainty relations are not always known to exist [14, 15].

In this work, we present an operational approach to quantifying incompatibility of any set of N noncommuting observables. We first observe that by definition, noncommuting observables do not have a complete set of common eigenkets. Therefore, some of the eigenstates, if not all, corresponding to different noncommuting observables must be non-orthogonal. We therefore suggest a measure that quantifies incompatibility of the observables as manifest in the non-orthogonality of their eigenstates. We will show that our measure applies

to any set of noncommuting observables (even if the observables commute on a subspace), and has the following desirable properties: it is zero when the observables commute, strictly greater than zero when they do not (note that the approach based on an uncertainty relation fails in this regard), and is maximum when they are mutually unbiased. We also obtain non-trivial upper bounds for any N noncommuting observables, and show that they are tight when $N \leq d+1$. We prove the latter by computing the measure exactly for any N mutually unbiased observables.

In order to define our measure of incompatibility, we adopt the following operational approach, best understood in the setting of quantum cryptography. We imagine a quantum key distribution (QKD) protocol between two observers, say, Alice and Bob, in presence of an eavesdropper employing an intercept-resend attack. Alice transmits quantum states drawn randomly from an ensemble (signal ensemble) S of equiprobable pure states, where the pure states are taken to be the eigenstates of the noncommuting observables whose incompatibility we wish to quantify. The eavesdropper performs a fixed measurement on every intercepted state (we will assume that all transmitted states are intercepted), replaces the original state with some other state based on the measurement outcome and sends it on to Bob. Our measure is defined as the complement of the accessible fidelity [31, 32] (the best possible average fidelity an eavesdropper can obtain) of the set S. Intuitively, this measure corresponds to the "amount of information" that is *inaccessible* to an eavesdropper.

For any given set $\Pi = \left\{\Pi^1, \Pi^2, ..., \Pi^N\right\}$ of N noncommuting observables acting on a Hilbert space $\mathscr{H}_d$ of dimension d, the signal ensemble is defined as a set of pure states $S(\Pi) = \left\{\Pi^i_j = |\psi^i_j\rangle\langle\psi^i_j|\right\}$ with $i = 1, ..., N$ and $j = 1, ..., d$, where $|\psi^i_j\rangle$ is the j^{th} eigenvector of the observable Π^i. As explained before, Alice transmits pure states Π^i_j drawn randomly from the set $S(\Pi)$ (probability of each state being equal to $1/Nd$), in presence of an eavesdropper employing an intercept-resend strategy comprising of some measurement (POVM) $\mathbf{M}$ and a state reconstruction map $\mathbf{A}$. First we define the notions of average and accessible fidelity [see Refs. [31, 32] for definitions in the more general case]. For a measurement $\mathbf{M} = \{M_a\}$, and a state reconstruction procedure $\mathbf{A} : a \to \sigma_a$ such that when the measurement outcome is a, the eavesdropper substitutes the intercepted state with some state σ_a and sends this state to Bob, the *average fidelity* of $S(\Pi)$ is given by:

$$F_{S(\Pi)}(\mathbf{M}, \mathbf{A}) \;=\; \frac{1}{Nd} \sum_{ija} \mathrm{Tr}\left(\Pi^i_j M_a\right) \mathrm{Tr}\left(\Pi^i_j \sigma_a\right), \qquad (2)$$

where $\frac{1}{Nd}\mathrm{Tr}\left(\Pi^i_j M_a\right)$ is the joint probability for the state Π^i_j and outcome a of the measurement, and $\mathrm{Tr}\left(\Pi^i_j \sigma_a\right)$ is the fidelity achieved in this case. The *optimal fidelity* is obtained by maximizing the average fidelity over all measurements and state reconstruction procedures:

$$F_{S(\Pi)} \;=\; \sup_{\mathbf{M}} \sup_{\mathbf{A}} \frac{1}{Nd} \sum_{ija} \mathrm{Tr}\left(\Pi^i_j M_a\right) \mathrm{Tr}\left(\Pi^i_j \sigma_a\right). \qquad (3)$$

The optimal fidelity represents the best possible average fidelity an eavesdropper can obtain. The measure of incompatibility of the noncommuting observables in the set Π is now defined as

$$Q(\Pi) \;=\; 1 - F_{S(\Pi)} \qquad (4)$$

It is clear from the definition that the measure is applicable even when the noncommuting observables $\left\{\Pi^i\right\}$ have one or more common eigenvectors. We will say that a set of observables Π_1 is more incompatible than another, say, Π_2, if the former takes on a larger Q value. It is interesting to note that the comparison holds regardless of the number of observables in each set and the dimension of the Hilbert space.

For any set Π of N noncommuting observables, $Q(\Pi)$ can in principle be computed but requires optimization which may be difficult to perform in general. Nevertheless, we give a simplified expression of a closely related quantity which might be useful to compute the measure for special classes of observables. We further note that our formalism is completely general in the sense that it can be applied to observables not all of which are commuting. Suppose we have a set $\mathfrak{S}$ of $\mathfrak{N}$ observables, in which some observables do not commute. From such a set one can always construct a minimal subset S of $N \leq \mathfrak{N}$ noncommuting observables with the property that any observable that is not in S must commute with at least one observable in S. For example, if $N = 1$, then it means that all observables in $\mathfrak{S}$ commute with each other, whereas $N = \mathfrak{N}$ implies that all observables in $\mathfrak{S}$ are noncommuting. Incompatibility of any set of observables is then defined as the incompatibility of the minimal noncommuting set obtained in this fashion.

The remainder of the paper is arranged as follows. We begin by proving two basic properties of Q (Proposition 1) and obtain the upper bounds (Theorem 1). We will then derive a simplified expression of a quantity closely related to optimal fidelity (Theorem 2) and use it to compute $Q(\Pi)$ exactly for any N mutually unbiased observables (Theorem 3). The result in Theorem 3 will imply that the upper bounds in Theorem 1 are tight. Finally we conclude with implications of these results in quantum cryptography and suggest future directions of research.

Proposition 1. *$Q = 0$ for commuting observables and $Q > 0$ when the observables do not commute.*

Proof. If the observables commute then they have a complete set of common eigenkets which form an orthonormal basis. Thus the minimal noncommuting set Π has only one element (any member of the commuting set), i.e., $N = 1$ and the set $S(\Pi)$ consists only of the common eigenkets which are mutually orthogonal. This implies that the optimal fidelity as defined by Eq. (3) is 1, and therefore $Q = 0$.

When the observables do not commute, then the minimal noncommuting set Π has at least two noncommuting observables. Then some of the eigenstates in $S(\Pi)$, if not all, belonging to different noncommuting observables must be non-orthogonal. Because non-orthogonal states cannot be distinguished perfectly, we have $F_{S(\Pi)} < 1$, and therefore, $Q > 0$. This completes the proof. □

We now obtain upper bounds on $Q(\Pi)$. The bounds are tight for mutually unbiased observables as will be shown in Theorem 3.

Theorem 1. *The following bounds hold for a set Π of N noncommuting observables acting on $\mathscr{H}_d$ with $\dim \mathscr{H}_d = d$:*

$$Q(\Pi) \;\leq\; \left(1-\frac{1}{N}\right)\left(1-\frac{1}{d}\right), \quad N \leq d+1 \tag{5}$$

$$Q(\Pi) \;\leq\; \frac{d-1}{d+1}, \quad N \geq d+1 \tag{6}$$

Before we get to the proof, we would like to point out that both bounds hold for any N. However, they are competing in the sense that one is better than the other depending on whether $N < d+1$ or $N > d+1$, and are equal when $N = d+1$.

Proof. We will first prove inequality (5). We will pick a measurement $\mathbf{M}$ and a state reproduction strategy $\mathbf{A}$ to obtain a lower bound on the average fidelity [Eq. (2)]; the result then follows from the definitions of optimal fidelity and $Q(\Pi)$. The measurement $\mathbf{M}$ that we choose is the standard von Neumann measurement in the eigenbasis of some observable $\Pi^k \in \Pi$. Thus the measurement $\mathbf{M} = \left\{\Pi_l^k = |\psi_l^k\rangle\langle\psi_l^k|\right\}_{l=1}^d$ consists of rank one orthogonal projection operators satisfying $\mathrm{Tr}\left(\Pi_j^k \Pi_l^k\right) = \delta_{jl}$ and $\sum_l \Pi_l^k = \mathbb{I}$. The state reconstruction map $\mathbf{A}$ reproduces the state Π_l^k if the outcome is l. With this, one can show that (details in the appendix),

$$F_{S(\Pi)}(\mathbf{M},\mathbf{A}) \;\geq\; \frac{N+d-1}{Nd} \tag{7}$$

Noting that, by definition, $F_{S(\Pi)} \geq F_{S(\Pi)}(\mathbf{M},\mathbf{A})$, we get

$$F_{S((\Pi)} \;\geq\; \frac{N+d-1}{Nd}. \tag{8}$$

Inequality (5) now follows from the definition of $Q(\Pi)$. To prove the upper bound in (6) we simply use a lower bound on the best possible average fidelity (accessible fidelity in the terminology of [31, 32]) obtained for any pure state ensemble $\mathscr{E} = \{|\psi_i\rangle, p_i\}$ [32],

$$F_{\mathscr{E}} \;\geq\; \frac{2}{d+1}$$

from which the result follows by definition of $Q(\Pi)$. □

Ideally we would like to compute $Q(\Pi)$ for any set Π. Unfortunately, there is no straightforward way to do the optimization in Eq. (3). Nevertheless, we hope to get some insight to the problem by obtaining a simplified form of the so called achievable fidelity [31, 32] obtained by maximizing the average fidelity over all state reconstruction strategies:

$$F_{S(\Pi)}(\mathbf{M}) \;=\; \sup_{\mathbf{A}} \frac{1}{Nd}\sum_{ija} \mathrm{Tr}\left(\Pi_j^i M_a\right)\mathrm{Tr}\left(\Pi_j^i \sigma_a\right). \tag{9}$$

As one can easily see, the optimal fidelity [Eq. (3)] can now be expressed as

$$F_{S(\Pi)} \;=\; \sup_{\mathbf{M}} F_{S(\Pi)}(\mathbf{M}) \tag{10}$$

We will assume, without any loss of generality that the POVM $\mathbf{M} = \{M_a\}$ consists only of rank one elements: $M_a = m_a\chi_a$, where $\chi_a = |\chi_a\rangle\langle\chi_a|$ is the density matrix corresponding to the normalized vector $|\chi_a\rangle$. For any such measurement one can calculate the achievable fidelity explicitly [31]:

$$F_{S(\Pi)}(\mathbf{M}) \;=\; \sum_a m_a \lambda\left(\Phi(\chi_a)\right) \tag{11}$$

where Φ is a trace non-increasing completely positive linear map defined for any density matrix ρ by

$$\Phi(\rho) \;=\; \frac{1}{Nd}\sum_i \Pi_j^i \rho \Pi_j^i \tag{12}$$

and $\lambda\left(\Phi(\rho)\right)$ is the largest eigenvalue of the Hermitian operator $\Phi(\rho)$.

Theorem 2. *For any $S(\Pi)$, and a measurement $\mathbf{M} = \{M_a = m_a\chi_a\}$ the achievable fidelity is given by*

$$F_{S(\Pi)}(\mathbf{M}) \;=\; \frac{1}{Nd}\sum_{ij} p(a)_j^i\, q(a)_j^i \tag{13}$$

where $p(a)_j^i = Tr\left(\Pi_j^i \chi_a\right)$, $q(a)_j^i = \langle\eta_a|\Pi_j^i|\eta_a\rangle$, and $|\eta_a\rangle$ is the eigenvector corresponding to the largest eigenvalue of $d\Phi(\chi_a)$.

Proof. Using Eq. (12) we can write $\Phi(\chi_a)$ as

$$\begin{aligned}\Phi(\chi_a) \;&=\; \frac{1}{Nd}\sum_{ij}\Pi_j^i\chi_a\Pi_j^i \\ &=\; \frac{1}{Nd}\sum_{ij}\mathrm{Tr}\left(\Pi_j^i\chi_a\right)\Pi_j^i\end{aligned} \tag{14}$$

Observe that $d\Phi(\chi_a)$ is a density matrix. Let's call it $\rho(\Phi,\chi_a)$, and the probabilities $\mathrm{Tr}\left(\Pi_j^i\chi_a\right) = p(a)_j^i$. Thus,

$$\rho(\Phi,\chi_a) \;=\; \frac{1}{N}\left(\rho_1+\rho_2+\cdots+\rho_N\right), \tag{15}$$

where $\rho_i = \sum_{j=1}^d p(a)_j^i \Pi_j^i$. Now suppose that $|\eta_a\rangle$ is the eigenvector of $\rho(\Phi,\chi_a)$ corresponding to the largest eigenvalue μ_a. Then,

$$\begin{aligned}\mu_a \;&=\; \langle\eta_a|\rho(\Phi,\chi_a)|\eta_a\rangle \\ &=\; \frac{1}{N}\sum_{ij} p(a)_j^i\, q(a)_j^i\end{aligned}$$

where $q(a)_j^i = \langle\eta_a|\Pi_j^i|\eta_a\rangle$. Noting that $d\Phi(\chi_a) = \rho(\Phi,\chi_a)$, the result follows from (11). □

We will now show that the upper bounds in Theorem 1 are tight for mutually unbiased observables. Mutually unbiased observables are those observables whose eigenvectors form mutually unbiased bases [33, 34, 36]. For N mutually unbiased observables, $\Pi^1, \Pi^2, ..., \Pi^N$, their eigenvectors satisfy:

$$\mathrm{Tr}\left(\Pi_j^i \Pi_k^i\right) = \delta_{jk} \quad (16)$$

$$\mathrm{Tr}\left(\Pi_j^i \Pi_l^k\right) = \frac{1}{d} \text{ when } i \neq k. \quad (17)$$

It is known that a complete set of $d+1$ mutually unbiased bases exist in prime and prime powered dimensions [34–36] . For other dimensions, however, the problem remains open.

Theorem 3. *Let $\Pi = \left\{\Pi^1, \Pi^2, ..., \Pi^N\right\}$ be a set of N mutually unbiased observables acting on $\mathscr{H}_d$ with $\dim \mathscr{H}_d = d$. Then,*

$$Q(\Pi) = \left(1 - \frac{1}{N}\right)\left(1 - \frac{1}{d}\right) \quad (18)$$

Proof. In this case $S(\Pi) = \left\{\Pi_j^i\right\}$, with $i = 1, ..., N$ and $j = 1, ..., d$, and the states Π_j^i satisfy Eqs. (16) and (17). Now Theorem 2 gives us an exact expression of the achievable fidelity for any set $S(\Pi)$ and a measurement $\mathbf{M} = m_a \chi_a$. By applying the Schwartz inequality to Eq. (13) one immediately obtains the following bound on the achievable fidelity:

$$F_{S(\Pi)}(\mathbf{M}) \leq \frac{1}{Nd} \sum_a m_a \sqrt{\sum_{ij} \left(p(a)_j^i\right)^2} \sqrt{\sum_{ij} \left(q(a)_j^i\right)^2} \quad (19)$$

We will now use the following lemma, proof of which is given in the appendix.

Lemma 1. *Let $|\phi\rangle \in \mathscr{H}_d$. Let $\left\{\Pi^i, i = 1, ..., N\right\}$, where $N \leq d+1$ be a set of mutually unbiased bases in $\mathscr{H}_d$. Let $t_j^i = \langle\phi|\Pi_j^i|\phi\rangle$, where Π_j^i is the j^{th} vector of the i^{th} basis. Then,*

$$\sum_{i=1}^{N} \sum_{j=1}^{d} \left(t_j^i\right)^2 \leq \frac{N+d-1}{d} \quad (20)$$

By application of Lemma 1 in inequality (19) we get,

$$F_{S(\Pi)}(\mathbf{M}) \leq \frac{N+d-1}{Nd^2} \sum_a m_a = \frac{N+d-1}{Nd} \quad (21)$$

where we have used $\sum_a m_a = d$ which follows from the fact that the elements $\{M_a\}$ of the POVM satisfy $\sum_a M_a = \mathbb{I}$. Noting that the upper bound (21) holds irrespective of the measurement $\mathbf{M}$, the optimal fidelity is therefore bounded by

$$F_{S(\Pi)} \leq \frac{N+d-1}{Nd}. \quad (22)$$

From the above inequality and the general lower bound on $F_{S(\Pi)}$ [inequality (8)] we therefore obtain ,

$$F_{S(\Pi)} = \frac{N+d-1}{Nd} \quad (23)$$

Eq. (18) now follows from the definition of $Q(\Pi)$. □

In summary, we have pointed out that uncertainty relations cannot, in general, be considered as a measure of incompatibility of noncommuting observables. This observation led us to propose a measure of incompatibility that applies to any set of noncommuting observables. The measure relies on two simple facts: When observables do not commute, at least some of their eigenstates must be non-orthogonal, and non-orthogonal quantum states cannot be perfectly distinguished. The measure is shown to satisfy the desired properties, namely, it is zero when the observables commute and strictly greater than zero when they do not. We have also obtained tight upper bounds for any N noncommuting observables and evaluated the measure exactly for mutually unbiased observables.

We note that the underlying physical principle defining our measure and the security of QKD protocols such as BB84 [25] and its generalizations [26–30] is the same. Thus the exact expression of incompatibility of any N mutually unbiased observables obtained here is expected to help analyze the security of such protocols. We further note that, in recent years entropic uncertainty relations have found applications in quantum cryptography [21, 22], information locking [23] and the separability problem [24]. We suspect that the results presented here will also be useful in the aforementioned contexts.

As a final comment, we feel that alternate measures of incompatibility of observables should be explored for reasons outlined in the introduction. While this paper suggests only one such measure, the idea behind is quite general and it is likely that similar quantities might serve as an equally good measure. Of course, it is hard to see how the difficulty of general optimization could be avoided.

Acknowledgments: SB thanks The Institute of Mathematical Sciences, Chennai, for supporting his visit in June 2012 when part of this work was completed. The authors are grateful to Bill Wootters for his comments on an earlier version of this work.

* Electronic address: email: som@bosemain.boseinst.ac.in
† Electronic address: email: prabhamd@imsc.res.in

[1] W. Heisenberg, Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik (The actual content of quantum theoretical kinematics and mechanics), Zeitschrift für Physik , 43, 172 (1927).
[2] H. P. Robertson, The uncertainty principle, Physical Review 34, 163 (1929).
[3] D. Deutsch, Uncertainty in quantum measurements, Physical Review Letters 50, 631 (1983).
[4] H. Maassen, and J. Uffink, Generalized entropic uncertainty relations, Physical Review Letters 60, 1103 (1988).
[5] Robertson [2] generalized Heisenberg's uncertainty relation [1] for any two observables A and B (in the chosen unit $\hbar = 1$):

$$\Delta A \Delta B \geq \frac{1}{2} |\langle\psi|[A,B]|\psi\rangle|, \quad (24)$$

where $\Delta X = \sqrt{\langle\psi|X^2|\psi\rangle - \langle\psi|X|\psi\rangle^2}$, $X \in \{A,B\}$ is the standard deviation resulting from measuring X on the quantum state $|\psi\rangle$. Deutsch pointed out that the above inequality is in general too weak except for canonically conjugate observables [3].

[6] I. I. Hirschmann, A note on etntropy, American Journal of Mathematics 79, 152 (1957).

[7] W. Beckner, Inequalities in Fourier analysis, Annals of Mathematics 102, 159 (1975).

[8] I. Bialynicki-Birula, and J. Mycielski, Uncertainty relations for information entropy in wave mechanics, Communications in Mathematical Physics 44, 129 (1975).

[9] I. Bialynicki-Birula, Entropic uncertainty relations, Physics Letters A 103, 253 (1984).

[10] I. D. Ivanovic, An inequality for the sum of entropies of unbiased quantum measurements, Journal of Physics A: Math. Gen. 25, 363 (1992).

[11] J. Sanchez, Entropic uncertainty and certainty relations for complementary observables, Physics Letters A 173, 233 (1993).

[12] J. Sanchez-Ruiz, Improved bounds in the entropic uncertainty and certainty relations for complementary observables, Physics Letters A 201, 125 (1995).

[13] J. Sanchez-Ruiz, Optimal entropic uncertainty relation in two-dimensional Hilbert space, Physics Letters A 244, 189 (1998).

[14] P. Mandayam, S. Wehner, and N. Balachandran, A transform of complementary aspects with applications to entropic uncertainty relations, Journal of Mathematical Physics 51, 082201 (2010).

[15] S. Wehner, and A. Winter, Entropic uncertainty relations—a survey, New Journal of Physics 12, 025009 (2010).

[16] S. Wehner, and A. Winter, Higher entropic uncertainty relations for anti-commuting observables, Journal of Mathematical Physics 49, 062105 (2008).

[17] H Maassen, A discrete entropic uncertainty relation, Quantum probability and applications V, Lecture Notes in Mathematics Volume 1442, 1990, pp 263-266 1990 - Springer.

[18] M. A. Ballester, and S. Wehner, Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases, Physical Review A 75, 022319 (2007).

[19] A. Azarchs, Entropic uncertainty relations for incomplete sets of mutually unbiased observables, arXiv preprint quant-ph/0412083, (2004).

[20] P. Hayden, D. Leung, P. Shor, and A. Winter, Randomizing quantum states: Constructions and applications, Communications in Mathematical Physics 250, 371 (2004).

[21] I. Damgaard, S. fehr, L. Salvail, and C. Schaffner, Cryptography in the bounded storage model, Proceedings of 46th IEEE FOCS, pp 449-458 (2005),

[22] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New Journal of Physics 11, 045018 (2009).

[23] D. DiVincenzo, M. Horodecki, D. Leung, J. Smolin, and B. Terhal, Locking classical correlations in quantum states, Physical Review Letters 92, 067902 (2004).

[24] O. Gühne, Characterizing entanglement via uncertainty relations, Physical Review Letters 92, 117903 (2004).

[25] C. H. Bennett, and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179 (1984).

[26] D. Bruss, Optimal eavesdropping in quantum cryptography with six states, Physical Review Letters 81, 3018 (1998).

[27] H. Bechmann-Pasquinucci, and N. Gisin, Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography, Physical Review A 59, 4238 (1999).

[28] H. Bechmann-Pasquinucci, and W. Tittel, Quantum cryptography using larger alphabets, Physical Review A 61, 062308 (2000).

[29] H. Bechmann-Pasquinucci, and A. Peres, Quantum cryptography with 3-state systems, Physical Review Letters 85, 3313 (2000).

[30] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of quantum key distribution using d-level systems, Physical Review Letters 88, 127902 (2002).

[31] C. Fuchs, and M. Sasaki, Squeezing quantum information through a classical channel: measuring the "quantumness" of a set of quantum states, Quantum Information & Computation 3, 377 (2003).

[32] C. Fuchs, On the quantumness of a Hilbert space, Quantum Information & Computation 4, 467 (2004).

[33] T. Durt, B. G. Englert, I. Bengtsson, K. Życzkowski, On mutually unbiased bases, International Journal of Quantum Information, 8, 535 (2010)

[34] I.D. Ivanovi´c, Geometrical description of quantal state determination. Journal of Physics A 14, 3241 (1981).

[35] W.K. Wootters and B.D. Fields. Optimal state-determination by mutually unbiased measurements. Ann. Physics, 191:363–381, 1989.

[36] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan. A new proof of the existence of mutually unbiased bases. Algorithmica, 34:512–528, 2002.

[37] U. Larsen, Superspace geometry: the exact uncertainty relationship between complementary aspects, Journal of Physics A: Math. Gen. 23, 1041 (1990).

[38] A. Klappenecker, and M. Rotteler, Mutually unbiased bases are complex projective 2-designs, Proceedings of the 2005 IEEE International Symposium on Information Theory (ISIT 05), 1740 (2005).

Appendix

Proof of Theorem 1.

Here we will derive inequality (7). For the choice of measurement **M** and the state reconstruction strategy **A** (as discussed in the text) the average fidelity [Eq. (2)] is given by,

$$\begin{aligned} F_{S(\Pi)}(\mathbf{M},\mathbf{A}) &= \frac{1}{Nd}\sum_{i,j,l}\left[\mathrm{Tr}\left(\Pi_j^i\Pi_l^k\right)\right]^2 \\ &= \frac{1}{N}+\frac{1}{Nd}\sum_{i\neq k,j,l}\left|\langle\psi_j^i|\psi_l^k\rangle\right|^4. \end{aligned} \quad (25)$$

Now the orthogonal states $\left\{|\psi_l^k\rangle\right\}_{l=1}^d$ form a basis of the Hilbert space $\mathscr{H}_d$. Therefore for any state $|\psi_j^i\rangle$,

$$\sum_{l=1}^{d}\left|\langle\psi_j^i|\psi_l^k\rangle\right|^2 = 1. \quad (26)$$

Furthermore, for $k\neq i$, we can write,

$$\left|\langle\psi_j^i|\psi_l^k\rangle\right|^2 = \frac{1}{d}+\Delta_{jl}^{ik} \;:\; k\neq i, \quad (27)$$

where Δ_{jl}^{ik} satisfies $-\frac{1}{d}\leq\Delta_{jl}^{ik}\leq 1-\frac{1}{d}$. From Eqs. (27) and (26) it follows that

$$\sum_{l=1}^{d}\Delta_{jl}^{ik} = 0 \;:k\neq i. \quad (28)$$

Substituting (27) in Eq. (25) and using Eq. (28), one obtains,

$$\begin{aligned} F_{S(\Pi)}(\mathbf{M},\mathbf{A}) &= \frac{1}{N}+\frac{1}{Nd}\sum_{i\neq k,j,l}\left(\frac{1}{d}+\Delta_{jl}^{ik}\right)^2 \\ &= \frac{1}{N}+\frac{N-1}{Nd}+\frac{1}{Nd}\sum_{i\neq k,j,l}\left(\Delta_{jl}^{ik}\right)^2 \\ &\geq \frac{1}{N}+\frac{N-1}{Nd}=\frac{N-d+1}{Nd}. \end{aligned}$$

Proof of Lemma 1

The following lemma will help us to prove Lemma 1.

Lemma 2. *Let V be a real vector space of dimension $(d-1)$ equipped with a inner product $\langle\psi|\phi\rangle=\sum_{k=1}^{d-1}a_kb_k$, where $\{a_k\}$ and $\{b_k\}$ are the components of the vectors $|\psi\rangle\in V$ and $|\phi\rangle\in V$ in some orthogonal basis. Let $\{|\psi_i\rangle\}_{i=1}^d$ be a set of linearly dependent vectors spanning V, with the property that $\langle\psi_i|\psi_i\rangle=\left(1-\frac{1}{d}\right)$ and $\langle\psi_i|\psi_j\rangle=-\frac{1}{d}$. Let $|\phi\rangle\in V$ such that $\sum_{i=1}^d\langle\psi_i|\phi\rangle=0$. Then $|\phi\rangle$ can be expressed as*

$$|\phi\rangle = \sum_{i=1}^{d}\lambda_i|\psi_i\rangle,$$

where $\lambda_i=\langle\phi|\psi_i\rangle$ are such that

$$\langle\phi|\phi\rangle = \sum_{i=1}^{d}\lambda_i^2.$$

Proof. As the set of vectors $\{|\psi_i\rangle\}_{i=1}^d$ span V we can write $|\phi\rangle$ as:

$$|\phi\rangle = \sum_{i=1}^{d}\lambda_i|\psi_i\rangle. \quad (29)$$

By explicitly computing the inner product of $|\phi\rangle$ with $|\psi_k\rangle$ we get,

$$\langle\psi_k|\phi\rangle = \lambda_k+\sum_{l=1}^{d}\lambda_l. \quad (30)$$

The given condition $\sum_{i=1}^d\langle\psi_i|\phi\rangle=0$, together with the above equation gives

$$(d+1)\sum_{k=1}^{d}\lambda_k = 0, \quad (31)$$

which implies that

$$\sum_{l=1}^{d}\lambda_l = 0. \quad (32)$$

Thus [from Eq. (30)],

$$\langle\psi_k|\phi\rangle = \lambda_k. \quad (33)$$

We will now prove that $\langle\phi|\phi\rangle=\sum_{i=1}^d\lambda_i^2$ by explicitly computing the squared norm:

$$\begin{aligned} \langle\phi|\phi\rangle &= \sum_{kj}\lambda_k\lambda_j\langle\psi_j|\psi_k\rangle \\ &= \left(1-\frac{1}{d}\right)\sum\lambda_k^2-\frac{1}{d}\sum_{j\neq k}\lambda_k\lambda_j \\ &= \sum\lambda_k^2. \end{aligned}$$

where to arrive at the last line we have used Eq. (32). □

To prove Lemma 1 we first note that the MUBs lie in the set of density matrices which itself is a convex subset of complex $d\times d$ Hermitian matrices. The set of complex $d\times d$ Hermitian matrices forms an d^2 - dimensional real vector space $\mathscr{V}$ equipped with the inner product $\mathrm{Tr}(AB)$ for any two vectors $A,B\in\mathscr{V}$. The density matrices are however, of unit trace and non-negative, and therefore lie in an $\left(d^2-1\right)$ - dimensional subspace of $\mathscr{V}$. This subspace is nothing but the vector space of all Hermitian matrices of unit trace.

For our purpose we will deal with the vector space of traceless Hermitian matrices $\mathscr{W}$ of dimension (d^2-1) with the inner product defined as $\mathrm{Tr}(AB)$ for any two traceless Hermitian matrices $A,B\in\mathscr{W}$. Thus a density matrix ρ will be

represented by $\tilde{\rho} = \rho - \frac{\mathbb{I}}{d}$. It is easy to check that the vectors belonging to different mutually unbiased bases are now orthogonal: That is,

$$\begin{aligned} \mathrm{Tr}\left(\tilde{\Pi}_j^i \tilde{\Pi}_l^k\right) &= \mathrm{Tr}\left(\Pi_j^i - \frac{\mathbb{I}}{d}\right)\left(\Pi_l^k - \frac{\mathbb{I}}{d}\right) \\ &= 0 \quad i \neq k \end{aligned}$$

Moreover, the vectors $\left\{\tilde{\Pi}_j^i = \Pi_j^i - \frac{\mathbb{I}}{d}\right\} : j = 1,...,d$ for a given i, span a $(d-1)$ dimensional subspace, say, $\mathscr{W}_i$. Thus when $(d+1)$ mutually unbiased bases exist, the vector space $\mathscr{W}$ can be decomposed into $(d+1)$ orthogonal subspaces; that is, $\mathscr{W} = \mathscr{W}_1 \oplus \cdots \oplus \mathscr{W}_{d+1}$. Therefore, $\tilde{\rho}$ can be expressed as

$$\tilde{\rho} = \sum_i \tilde{\rho}_i,$$

where $\tilde{\rho}_i \in \mathscr{W}_i$.

Let $r_j^i = \mathrm{Tr}\left(\tilde{\rho}\tilde{\Pi}_j^i\right)$, where the r_j^is' determine the projection of $\tilde{\rho}$ onto the subspace $\mathscr{W}_i$ and are related to the probabilities $t_j^i = \mathrm{Tr}\left(\Pi_j^i \rho\right), j = 1,...,d$, when ρ is measured in the Π^i basis via the following relation:

$$r_j^i = t_j^i - \frac{1}{d}.$$

Note that r_j^is' satisfy

$$\sum_{j=1}^{d} r_j^i = 0,$$

by virtue of the fact that $\sum_j t_j^i = 1$. Now observe that $r_j^i = \mathrm{Tr}\left(\tilde{\rho}\tilde{\Pi}_j^i\right) = \mathrm{Tr}\left(\tilde{\rho}_i\tilde{\Pi}_j^i\right)$. This follows from the facts that $\tilde{\rho} = \sum_i \tilde{\rho}_i$, and $\mathrm{Tr}\left(\tilde{\rho}_k\tilde{\Pi}_j^i\right) = 0 : k \neq i$. Therefore, by Lemma 2 we can write $\tilde{\rho}_i$ as,

$$\tilde{\rho}_i = \sum_j r_j^i \tilde{\Pi}_j^i.$$

Once again by Lemma 2, we obtain

$$\mathrm{Tr}\left(\tilde{\rho}_i^2\right) = \sum_j \left(r_j^i\right)^2.$$

Since $\mathrm{Tr}\left(\tilde{\rho}\right)^2$ is simply the sum of the squares of the lengths of the components of $\tilde{\rho}$ in the orthogonal subspaces $\mathscr{W}_i$, we have,

$$\mathrm{Tr}\left(\tilde{\rho}^2\right) = \sum_{ij} \left(r_j^i\right)^2.$$

For any density matrix ρ, the right hand side can be readily evaluated:

$$\begin{aligned} \sum_{ij} \left(r_j^i\right)^2 &= \sum_{ij} \left(t_j^i\right)^2 - \sum_i \frac{1}{d} \\ &= \sum_i \left(\sum_j \left(t_j^i\right)^2 - \frac{1}{d}\right). \end{aligned} \tag{34}$$

Observe that the quantity $\left(\sum_j \left(t_j^i\right)^2 - \frac{1}{d}\right) = \sum_j \left(r_j^i\right)^2 \geq 0$.

When ρ corresponds to a pure state, then

$$\begin{aligned} \mathrm{Tr}\left(\tilde{\rho}^2\right) &= \mathrm{Tr}\left(\rho - \frac{\mathbb{I}}{d}\right)^2 \\ &= 1 - \frac{1}{d}. \end{aligned}$$

To arrive at our result we simply note that when $i = 1,...,N$, where $N \leq d+1$,

$$\sum_{i=1}^{N}\sum_{j=1}^{d} \left(r_j^i\right)^2 \leq 1 - \frac{1}{d}. \tag{35}$$

Using Eqs. (34) and (35) we therefore obtain,

$$\sum_{i=1}^{N}\sum_{j=1}^{d} \left(t_j^i\right)^2 \leq \frac{N+d-1}{d}.$$

The equality is reached only when the pure state lies in the union of the subspaces $\mathscr{W}_i$, $i = 1,...,N$. Also note that when $N = d+1$ we get back the known result [37, 38]. This completes the proof of Lemma 1.